AUTOMORPHISMS OF A CERTAIN SKEW POLYNOMIAL RING OF DERIVATION TYPE

ISAO KIKUMASA

1. Introduction. Throughout this paper, all rings have the identity 1 and ring homomorphisms are assumed to preserve 1. We use p to denote a prime integer and F to denote a field of characteristic p. For an element α in F, we set

$$A = F[x]/(x^p - \alpha)F[x].$$

Moreover, by D and R, we denote the derivation of A induced by the ordinary derivation of F[x] and the skew polynomial ring A[X;D] where aX = Xa + D(a) $(a \in A)$, respectively (cf. [2]).

In [3], R. W. Gilmer determined all the B-automorphisms of B[X] for any commutative ring B. Since then, some extensions or generalizations of his results have been obtained ([1], [2] and [5]). As to the characterization of automorphisms of skew polynomial rings, M. Rimmer [5] established a thorough result in case of automorphism type, while M. Ferrero and K. Kishimoto [2], among others, have made some progress in case of derivation type.

But, [2] is a study on *B*-automorphisms of $B[X;\delta]$ in case that *B* is a ring with a derivation δ satisfying the condition $\delta(N) \subset N$ where *N* is the union of all nilpotent ideals of B. Moreover, in that study, it is shown that this condition is fulfilled in the following cases: *B* is torsion free; *B* is semiprime. However, apart from these cases, we can find no information about this condition. Hence the results on [2] can not necessarily be applied to rings of characteristic *p*. In particular, we can never apply it to the ring $F[x]/(x^p)F[x]$ with the derivation *D* which is useful in studies of algebra.

On the other hand, for the algebra A, Jacobson [4, p. 190] mentions a certain kind of A-automorphisms of R in case that $x^p - \alpha$ is irreducible in F[x]. In this case there exists no another kind of A-automorphisms of R, which can be easily seen from our theorem or [2]. However, if $x^p - \alpha$ is not irreducible then A is isomorphic to $F[x]/(x^p)F[x]$, hence the problem to determine all the A-automorphisms of R has never been solved except in the case that A is a field.

The aim of this paper is to solve this problem and, as a result, to show an automorphism whose type is quite different from ones in [1], [2], [3] and [5].

To study this object, we consider the following conditions for the A-linear map ϕ of R to itself defined by

(#)
$$X^k \to \left(\sum_{i=0}^n X^i a_i\right)^k$$
, $k = 0, 1, 2, \dots (n \ge 2, a_n \ne 0)$.

Received March 1, 1989.

A.M.S. (1980) subject classification: 16A21, 16A05.

(In case n = 1, see Remark 2.)

(a-i)
$$a_1 = 1$$
.

(a-ii)
$$a_i = 0$$
 for all $i \in \{j : 2 \le j \le n \text{ and } p \nmid j\}$.

Assume that (a-ii) is fulfilled. Then, it follows from $n \ge 2$ and $a_n \ne 0$ that $p \mid n$. Hence there exist integers s and t which satisfy ps = n and $pt \le s < p(t+1)$. Thus the following conditions can be considered.

(b-i)
$$D^{p-1}(a_p) + 1 \neq 0$$
.

(b-ii)
$$D^{p-1}(a_{p^2i}) + a_{pi}^p = 0$$
 for all $i \in \{j : 1 \le j \le t\}$.

(b-iii)
$$a_{ni}^p = 0$$
 for all $i \in \{j : t+1 \le j \le s\}$.

(b-iv)
$$D^{p-1}(a_{pi}) = 0$$
 for all $i \in \{j : 2 \le j \le s \text{ and } p \nmid j\}$.

2. The main theorem. Our study starts by stating our main theorem.

THEOREM 1. The map ϕ is an A-automorphism of R if and only if (a-i), (a-ii), and (b-i)–(b-iv) hold. Furthermore in this case, the inverse map ϕ^{-1} of ϕ is induced by

$$X^{k} \longrightarrow \left(X + \sum_{j=0}^{s} X^{pj} b_{pj}\right)^{k}, \quad k = 0, 1, 2, \dots$$

where

$$b_{pj} = \sum_{i=j}^{s} (-1)^{i-j+1} \binom{i}{j} (D^{p-1}(a_0) + a_0^p)^{i-j} (D^{p-1}(a_p) + 1)^{-i} a_{pi}$$

for each j. In particular, every A-automorphism ψ is necessarily of the above form.

To prove this theorem, we need several lemmas.

LEMMA 2. Let i, j and k be non-negative integers.

(1) If 0 < i < pk and $p \nmid i$ then

$$\binom{pk}{i} \equiv 0 \pmod{p}.$$

(2) If $0 \le j \le k$ then

$$\binom{pk}{pj} \equiv \binom{k}{j}^p \equiv \binom{k}{j} \pmod{p}.$$

Proof. Since F is of characteristic p, we have the following equalities in F[X] by the binomial theorem:

$$(1+X)^{pk} = \sum_{h=0}^{pk} \binom{pk}{h} X^h,$$

$$(1+X)^{pk} = \{(1+X)^k\}^p = \left(\sum_{h=0}^k \binom{k}{h} X^h\right)^p = \sum_{h=0}^k \binom{k}{h}^p X^{ph}$$

and

$$(1+X)^{pk} = \{(1+X)^p\}^k = (1+X^p)^k = \sum_{h=0}^k \binom{k}{h} X^{ph}.$$

Hence we have (1) and (2) by comparing the coefficients of X^i and X^{pj} , respectively.

LEMMA 3. Let B be a commutative algebra over the prime field GF(p) and δ a derivation of B such that $\delta^p = 0$. Assume that $\delta(z) = 1$ for some z in B. Then (1) and (2) hold.

- (1) The map $X \to \sum_{i=0}^n X^i b_i$ $(b_i \in B, n \ge 1, b_n \ne 0)$ induces a B-endomorphism of $B[X;\delta]$ if and only if
 - (i) $b_1 = 1$ and
 - (ii) $b_i = 0$ for all $i \in \{j : 2 \le j \le n \text{ and } p \nmid j\}$.

When this is the case, the image of X takes the form

$$X + \sum_{i=0}^{s_0} X^{pi} b_{pi}$$

where s_0 is an integer such that $ps_0 = n$ if $n \ge 2$, and $s_0 = 0$ if n = 1.

(2) Let $I = \{b \in B : \delta(b) = 0\}$. Then, the center of $B[X;\delta]$ coincides with $I[X^p]$, the polynomial ring in X^p over the algebra I. Moreover, $B[X^p]$ is the unique maximal commutative subalgebra of $B[X;\delta]$ containing B.

Proof. Let ϕ_0 be the *B*-linear map of $B[X;\delta]$ to itself induced by

$$X^k \longrightarrow \left(\sum_{i=0}^n X^i b_i\right)^k, \quad k = 0, 1, 2, \dots$$

We note that ϕ_0 is a *B*-endomorphism of $B[X;\delta]$ if and only if

$$b\phi_0(X) = \phi_0(X)b + \delta(b)$$

for any b in B. From this, it is easily seen that ϕ_0 is a B-endomorphism of $B[X;\delta]$ if and only if the following equalities hold for any b in B (cf. [2, (1.1)]).

$$\sum_{k=0}^{n} \delta^{k}(b)b_{k} = b_{0}b + \delta(b),$$

$$\sum_{k=i-1}^{n} \binom{k}{i-1} \delta^{k-(i-1)}(b)b_{k} = b_{i-1}b \quad (i \ge 2).$$

Assume that ϕ_0 is a *B*-endomorphism of $B[X;\delta]$. Since $\delta(z)=1$, $\delta^k(z)=0$ ($k \ge 2$). Substitute here z for b in the above equalities. Then, the condition (i) will be easily seen from the first equality. Moreover, from the second equality, we have

$$zb_{i-1} + i\delta(z)b_i = b_{i-1}z.$$

This enables us to see (ii).

Conversely, assume that (i) and (ii) are satisfied. If k > i - 1 and $p \mid k$ then

$$\binom{k}{i-1}\delta^{k-(i-1)}(b) = 0$$

for any b in B by Lemma 2 and our assumption $\delta^p = 0$. On the other hand, if k > i-1 and $p \nmid k$ then $b_k = 0$ by (ii). This shows that the above second equality holds. Moreover, noting $b_1 = 1$ (i), we have the first equality in a similar way. Thus (1) has been proved.

To see the assertion (2), C will denote the center of $B[X : \delta]$. First, we shall prove that $I[X^p] \subset C$. Let

$$f(X) = \sum_{i=0}^{k} X^{pi} \epsilon_{pi} \quad (\epsilon_{pi} \in I)$$

be an arbitrary element in $I[X^p]$. Then, f(X) commutes with every element in B. Indeed, it is easily seen that

$$bX^{p} - X^{p}b = \sum_{j=0}^{p-1} X^{j} \binom{p}{j} \delta^{p-j}(b)$$

for any b in B. Then, it follows from Lemma 2(1) and our assumption $\delta^p = 0$ that $bX^p = X^pb$ for any b in B. Also, since $\delta(\epsilon_{pi}) = 0$ $(0 \le i \le k)$, f(X) commutes with X and so does with every element of $B[X;\delta]$. This means that $I[X^p] \subset C$.

Conversely, let $g(X) = \sum_{i=0}^{k} X^{i} c_{i}$ $(k \ge 0, c_{k} \ne 0)$ belong to C. Since

$$0 = g(X)X - Xg(X) = \sum_{i=0}^{k} X^{i}\delta(c_{i}),$$

it follows that $\{c_i\}$ is contained in *I*. Hence it is enough to show that $\sum_{i \in T} X^i c_i = 0$ where $T = \{i : 0 \le i \le k \text{ and } p \nmid i\}$. Suppose that $\sum_{i \in T} X^i c_i \ne 0$ and let *m* be the maximal element in $\{i \in T : c_i \ne 0\}$. Then, since $X^p \in C$, we have

$$bg(X) - g(X)b = b\left(\sum_{i \in T} X^i c_i\right) - \left(\sum_{i \in T} X^i c_i\right)b \quad (b \in B)$$

which is equal to zero. As is easily seen, the coefficient of X^{m-1} is $m\delta(b)c_m$. Hence we have $mc_m = 0$ by taking z as b. Since $p \nmid m$ and $c_m \neq 0$, this is a contradiction.

Moreover, since $bX^p = X^pb$ for any b in B, $B[X^p]$ is a commutative subalgebra of $B[X;\delta]$ containing B. Let S be a commutative subalgebra of $B[X;\delta]$ containing B. Then, for every element $g(X) = \sum_{i=0}^k X^i c_i$ in S, we have bg(X) = g(X)b ($b \in B$). Hence one can easily see that $g(X) = \sum_{i=0}^h X^{pi} c_{pi}$ for some integer $h \ge 0$ as in the above argument. This shows that $S \subset B[X^p]$, and hence $B[X^p]$ is the unique maximal commutative subalgebra of $B[X;\delta]$ containing B.

The following lemma is a special case of the formula (31) of [4, p. 189].

LEMMA 4. Let E be an F-algebra. For given a and b in E, define $b^{(k)}$ $(0 \le k \le p-1)$ inductively as follows:

$$b^{(0)} = a \text{ and } b^{(k)} = [b^{(k-1)}, b]$$

where [c,d] = cd - dc $(c,d \in E)$. If a commutes with all $b^{(k)}$ $(1 \le k \le p-2)$, then

$$(a+b)^p = a^p + b^p + b^{(p-1)}$$
.

By D^* , we denote the derivation of R induced by D, that is,

$$D^* \left(\sum_{i=0}^k X^i b_i \right) = \sum_{i=0}^k X^i D(b_i)$$

for each $\sum_{i=0}^{k} X^{i}b_{i}$ in R. Then, we can apply the above lemma to $a = \sum_{i=0}^{s} X^{pi}a_{pi}$ and b = X in the algebra R to obtain

(*)
$$(X+a)^p = X^p + D^{*p-1}(a) + a^p,$$

because

$$b^{(1)} = [a, X] = D^*(a)$$
 and $b^{(k)} = D^{*k}(a) = \sum_{i=0}^{s} X^{pi} D^k(a_{pi})$ $(0 \le k \le p-1)$

which are contained in the maximal commutative subalgebra $A[X^p]$ of R by Lemma 3. Moreover, we have

$$a^{p} = \sum_{i=0}^{s} X^{P^{2}i} a_{pi}^{p}$$

which is used in the subsequent study.

Proof of Theorem 1. Let ϕ be the A-linear map induced by (#) and C the center of R. Then $C = F[X^p]$ by Lemma 3. Assume that the map ϕ is an A-endomorphism of R. Then, by Lemma 3, (a-i) and (a-ii) are satisfied and we can write

$$\phi(X) = X + \sum_{i=0}^{s} X^{pi} a_{pi}.$$

Hence, by (*), we have

$$\phi(X^p) = \phi(X)^p$$

$$= X^p + \sum_{i=0}^s X^{pi} D^{p-1}(a_{pi}) + \sum_{i=0}^s X^{p^2 i} a_{pi}^p.$$

We write here

$$\phi(X^p) = \sum_{i=0}^n X^{pi} \alpha_{pi}.$$

Obviously there hold the following equalities:

$$\alpha_{pi} = 0 \quad \text{for all } i \in \{j : s < j < ps = n \text{ and } p \nmid j\};$$

$$\alpha_p = D^{p-1}(a_p) + 1;$$

$$(**) \quad \alpha_{p^2i} = D^{p-1}(a_{p^2i}) + a_{pi}^p \quad \text{for all } i \in \{j : 0 \le j \le t\};$$

$$\alpha_{p^2i} = a_{pi}^p \quad \text{for all } i \in \{j : t + 1 \le j \le s\};$$

$$\alpha_{pi} = D^{p-1}(a_{pi}) \quad \text{for all } i \in \{j : 2 \le j \le s \text{ and } p \nmid j\}.$$

Then, we note that $D^{p-1}(a_{pi})$ and a_{pi}^p $(0 \le i \le s)$ are in F. Hence, the α_{pi} are contained in F. This shows that the A-endomorphism ϕ induces an F-endomorphism of C.

Now, assume that the map ϕ is an A-automorphism of R. Then, the A-automorphism ϕ induces uniquely an F-automorphism of C such that

$$X^p \longrightarrow \sum_{i=0}^n X^{pi} \alpha_{pi}.$$

As is well-known (cf. [3, p. 331, Theorem 3]),

$$Y \longrightarrow \sum_{i=0}^{n} Y^{i} \alpha_{pi}$$

induces an *F*-automorphism of the commutative polynomial ring F[Y] if and only if $\alpha_p \neq 0$ and $\alpha_{pi} = 0$ for all $i \geq 2$. It follows therefore that (b-i)–(b-iv) are fulfilled.

Next, we shall show the converse. Assume that the conditions (a-i)—(a-ii) and (b-i)—(b-iv) are fulfilled. Then, combining (a-i)—(a-ii) with the result of Lemma 3, we see that the map ϕ is an A-endomorphism of R and

$$\phi(X) = X + \sum_{i=0}^{s} X^{pi} a_{pi}.$$

Hence $\phi(X^p) = \alpha_0 + X^p \alpha_p$ by (b-i)–(b-iv) and (**). Thus, the A-endomorphism ϕ induces an F-automorphism ϕ_c of $C = F[X^p]$ such that

$$X^p \longrightarrow \alpha_0 + X^p \alpha_n$$

and the inverse map ϕ_c^{-1} of ϕ_c satisfies

$$\phi_c^{-1}(X^p) = -\alpha_0 \alpha_p^{-1} + X^p \alpha_p^{-1}.$$

For the A-endomorphism ϕ , there exists an A-endomorphism ψ of R such that

$$\psi(X) = X + \sum_{i=0}^{s} X^{pi} b_{pi}$$
 and $\phi \psi(X) = X$.

Indeed, by Lemma 3, the map

$$X \longrightarrow X + \sum_{i=0}^{s} X^{pi} b_{pi}$$

induces an A-endomorphism of R for any b_{pi} in A. Putting $Y = \alpha_0 + X^p \alpha_p$, we have

$$\phi\psi(X) - X = \sum_{i=0}^{s} X^{pi} a_{pi} + \sum_{i=0}^{s} (\alpha_0 + X^p \alpha_p)^i b_{pi}$$

$$= \sum_{i=0}^{s} \left[\left\{ (Y - \alpha_0) \alpha_p^{-1} \right\}^i a_{pi} + Y^i b_{pi} \right]$$

$$= \sum_{j=0}^{s} Y^j \left\{ \sum_{i=j}^{s} (-1)^{i-j} \binom{i}{j} \alpha_0^{i-j} \alpha_p^{-i} a_{pi} + b_{pj} \right\},$$

because of the commutativity of the center $C = F[X^p]$ of R. Therefore, an A-endomorphism ψ with

$$b_{pj} = \sum_{i=j}^{s} (-1)^{i-j+1} \binom{i}{j} \alpha_0^{i-j} \alpha_p^{-i} a_{pi} \quad (0 \le j \le s)$$

has the property $\phi\psi(X) = X$.

We shall now prove that $\psi\phi(X)=X$. We define β_{pi} as (**), using b_{pi} in place of a_{pi} . Then, the restriction ψ_c of ψ to $F[X^p]$ maps X^p to $\sum_{i=0}^n X^{pi}\beta_{pi}$. Since $\phi\psi(X)=X$, we have $\phi\psi(X^p)=X^p$ and so $\phi_c\psi_c(X^p)=X^p$. Thus,

$$\psi_c(X^p) = \sum_{i=0}^n X^{pi} \beta_{pi} = \phi_c^{-1}(X^p) = -\alpha_0 \alpha_p^{-1} + X^p \alpha_p^{-1}.$$

Hence, we obtain

$$\beta_0 = -\alpha_0 \alpha_p^{-1}, \quad \beta_p = \alpha_p^{-1} \quad \text{and} \quad \psi(X^p) = \beta_0 + X^p \beta_p.$$

Now we are in a position to complete the proof. Indeed, we have

$$\psi\phi(X) - X = \psi\left(X + \sum_{i=0}^{s} X^{pi} a_{pi}\right) - X$$

$$= \sum_{i=0}^{s} X^{pi} b_{pi} + \sum_{i=0}^{s} (\beta_0 + X^p \beta_p)^i a_{pi}$$

$$= \sum_{j=0}^{s} X^{pj} \left\{b_{pj} + \sum_{i=j}^{s} \binom{i}{j} \beta_0^{i-j} \beta_p^j a_{pi}\right\}$$

$$= \sum_{j=0}^{s} X^{pj} \left\{b_{pj} + \sum_{i=j}^{s} (-1)^{i-j} \binom{i}{j} \alpha_0^{i-j} \alpha_p^{-i} a_{pi}\right\}$$

$$= 0$$

which shows, together with $\phi\psi(X)=X$, that ϕ is an A- automorphism of R and $\psi=\phi^{-1}$.

3. Remarks and examples. In the rest of this paper, let y be the image of x in A by the canonical homomorphism from F[x] to

$$A = F[x]/(x^p - \alpha)F[x].$$

We shall now present some interesting results which are obtained from our theorem.

Remark 1. Since each a_{pi} is an element in A, we can write

$$a_{pi} = \sum_{k=0}^{p-1} y^k \gamma_{pi,k} \quad (\gamma_{pi,k} \in F).$$

Then

$$a_{pi}^p = \sum_{k=0}^{p-1} \alpha^k \gamma_{pi,k}^p$$
 and
$$D^{p-1}(a_{pi}) = (p-1)! \gamma_{pi,p-1} = -\gamma_{pi,p-1}$$

by Wilson's Theorem. Thus, one can replace the condition (b-i)–(b-iv) with the following:

$$\begin{aligned} &\text{(b-ii)'} & \gamma_{p,p-1} \neq 1; \\ &\text{(b-ii)'} & \gamma_{p^2i,p-1} = \sum_{k=0}^{p-1} \alpha^k \gamma_{pi,k}^p & \text{for all } i \in \{j: 1 \leq j \leq t\}; \\ &\text{(b-iii)'} & \sum_{k=0}^{p-1} \alpha^k \gamma_{pi,k}^p = 0 & \text{for all } i \in \{j: t+1 \leq j \leq s\}; \\ &\text{(b-iv)'} & \gamma_{pi,p-1} = 0 & \text{for all } i \in \{j: 2 \leq j \leq s \text{ and } p \nmid j\}. \end{aligned}$$

Obviously in case $\alpha=0$, these relations show that whether or not the A-endomorphism ϕ of R is an A-automorphism depends only on the coefficients $\gamma_{pi,p-1}$ of y^{p-1} and constant terms $\gamma_{pi,0}$ of a_{pi} $(1 \le i \le s)$. Therefore the coefficients $\gamma_{pi,k}$ of intermediate terms y^k $(1 \le k \le p-2)$ can be taken freely, and so if p is an odd prime (i.e., $p \ne 2$) then one can easily make different A-automorphisms of R from any given A-automorphism of R. This also means that there exist at least $|F|^{(p-2)s}$ A-automorphisms of R whose image of X is of degree n=ps, where |F| is the cardinal number of the field F.

Remark 2. In case n=1, M. Ferrero and K. Kishimoto [2, Lemma 2] have shown that if B is a ring and δ is a derivation of B, then the map $X \to b_0 + Xb_1$ induces a B-automorphism of $B[X;\delta]$ if and only if b_1 is a central unit and

$$b_0b - bb_0 = \delta(b)(b_1 - 1)$$
 for all $b \in B$.

Noting D(y) = 1, one will easily see the map $X \to a_0 + Xa_1$ induces an A-automorphism of R if and only if $a_1 = 1$. Thus, one can consider Theorem 1 to contain the case n = 1.

Examples. Let $\alpha = 0$ i.e., $A = F[x]/(x^p)F[x]$.

1. Suppose that p=2. Let maps ϕ_1 and ϕ_2 be A-endomorphisms of R induced by

$$X \longrightarrow X + X^2y$$
 and $X \longrightarrow X + X^2y\beta$ $(\beta \neq 1 \in F)$

respectively. Then, by the condition (b-i) in Theorem 1 (or the condition (b-i)' in Remark 1), ϕ_1 is not an A-automorphism of R. But ϕ_2 is an A-automorphism of R by Theorem 1. When this is the case, then

$$\phi_1(X^2) = 0$$
 and $\phi_2^{-1}(X) = X - X^2 y(\beta + 1)^{-1} \beta$.

2. We shall make a note about an interesting property of the coefficients of

$$\phi(X) = \sum_{i=0}^{n} X^{i} a_{i}.$$

It is easily seen by the condition (b-ii) (or (b-ii)') that a_{pi} don't have to be nilpotent for all $i \ge 2$, though the map ϕ is an A-automorphism of R. Actually, we know by Theorem 1 that the map

$$X \longrightarrow X + X^p + X^{p^2} y^{p-1}$$

induces an A-automorphism of R, though $a_p = 1$ is not nilpotent. This shows that there exists an automorphism whose form is quite different from ones known before now, because all results in [1], [2], [3] and [5] have shown that a_i ($i \ge 2$) must be nilpotent for the map $X \to \sum_{i=0}^n X^i a_i$ to induce a B-automorphism of a commutative or skew polynomial ring over a ring B.

Acknowledgements. The author is grateful to Professor T. Nagahara for his valuable help during the preparation of this paper. Also, the author would like to express his indebtedness and gratitude to Professors S. Ikehata and H. Kaneta for their helpful suggestions and comments.

REFERENCES

- 1. D. B. Coleman and E. E. Enochs, *Isomorphic polynomial rings*, Proc. Amer. Math. Soc. 27 (1971), 247–252.
- M. Ferrero and K. Kishimoto, On automorphisms of skew polynomial rings of derivation type, Math. J. Okayama Univ. 22 (1980), 21–26.
- 3. R. W. Gilmer, R-automorphisms of R[X], Proc. London Math. Soc. 18 (1968), 328-336.
- N. Jacobson, Lectures in abstract algebra, Vol. III (Van Nostrand, Toronto/New York/London, 1964).
- 5. M. Rimmer, Isomorphisms between skew polynomial rings, J. Austral. Math. Soc. 25 (1978), 314–321.
- 6. J. Riordan, Combinatorial identities (John Wiley & Sons, New York/London/Sydney, 1968).

Okayama University, Okayama, Japan